類数が3で割れる二次体の特徴づけ (代数的整数論とその周辺)

AUTHOR(S):

岸, 康弘

CITATION:

岸, 康弘. 類数が3で割れる二次体の特徴づけ(代数的整数論とその周辺). 数理解析研究所講究録 1998, 1026: 151-155

ISSUE DATE:

1998-02

URL:

http://hdl.handle.net/2433/61760

数理解析研究所講究録
1026巻 1998年 151-155

類数が3で割れる二次体の特徴づけ

(東京都立大学理学研究科博士課程) 岸 康弘 (Yasuhiro Kishi)

§0 序

どのような整数 N に対しても, 類数が N で割れる虚二次体が無限に存在することは古くから知られていた (Nagel [6]). また実二次体についても, $N=3$ の場合に, そのようなものが無限に存在することが示された (Honda [4]). 以降, 類数が 3 で割れる二次体の無限族がいくつか与えられている (Hartung [2], Brinkhuis [1], Ohta [7] など). 今回, 類数が 3 で割れる二次体を二つのパラメータで特徴づけ, さらに, その上の 3 次不分岐アーベル拡大を与える 3 次多項式も特徴づけた (Kishi-Miyake[5]). §1 では主定理を述べるが, 証明は省略する. §2 では既存の無限族と主定理との関連について述べる. また, 実二次体 $\mathbb{Q}(\sqrt{D})$ と虚二次体 $\mathbb{Q}(\sqrt{-3D})$ との関連についても少し述べておく.

§1 主定理

有理数体 $\mathbb{Q}$ 上の 3 次多項式 $g(Z)$ で以下の条件を満たすものを考える:

$$g(Z)=Z^3-uwZ-u^2, \quad u,\ w\in\mathbb{Z}$$

但し, u と w は互いに素であり, $4uw^3-27u^2$ は完全平方数でなく, さらに条件

(i) $3\nmid w$

(ii) $3\mid w,\ uw\not\equiv 3 \pmod 9,\ u\equiv w\pm 1 \pmod 9$

(iii) $3\mid w,\ uw\equiv 3 \pmod 9,\ u\equiv w\pm 1 \pmod{27}$

のうち, いずれか一つを満たす.

この多項式 $g(Z)$ の判別式 D は

$$D = u^2 d, \qquad d = 4uw^3 - 27u^2$$

である. したがって, $g(Z)$ が $\mathbb{Q}$ 上既約ならば, 最小分解体は $\mathbb{Q}$ 上 S_3- 拡大で, その最小分解体は二次体 $k = \mathbb{Q}(\sqrt{d})$ を含む.

主定理. 上の諸条件を満たす $g(Z)$ が $\mathbb{Q}$ 上既約ならば, $g(Z) = 0$ の根は二次体 k 上 3 次の不分岐アーベル拡大を与える. 逆に, 類数が 3 で割れる二次体 k とその上の 3 次不分岐アーベル拡大はすべてこの形で得られる.

注意. 証明の方針は, 3 次多項式の根が作る体で, すべての素数が完全分岐しないように, その 3 次多項式の係数の条件を決定していく. 従って, 二次体 k が実であるか虚であるかに関係なく結果が得られる.

§2 部分族

まず, いくつかの無限部分族を紹介する.

例 1. (Honda [4]) 二つの整数 m と n が次を満たすとする : (i) $(m, 3n) = 1$, (ii) $d := 4m^3 - 27n^2$ は平方数にならない, (iii) $m = (n + a^2)/a$ $(a \in \mathbb{Z})$ の形で表されない. このとき, $\mathbb{Q}(\sqrt{d})$ の類数は 3 で割れる.

証明. 主定理で $u = n^2$, $w = m$ とすれば, この場合が得られる. □

例 2. (Hartung [2]) 平方因子を持たない整数 m が次を満たすとする : (i) $m \equiv 7 \pmod{12}$, (ii) $m = (n^2 - 4)/27$ $(n \in \mathbb{Z})$ の形で表される. このとき, $\mathbb{Q}(\sqrt{-m})$ の類数は 3 で割れる.

証明. この場合は、主定理で $u = n^2$, $w = 3$ としたものである. □

例 3. (Brinkhuis [1]) 整数 m が $n^3 - n^2$ $(n \in \mathbb{Z})$ の形で表されないとする. そのとき, $\mathbb{Q}(\sqrt{-4m - 27m^2})$ の類数は 3 で割れる.

証明. これは, 主定理で $u = m$, $w = -1$ としたものである. □

例 4. 互いに素な二つの整数 u と w を次のようにとる：(i) $d := 4uw^3 - 27u^2$ は平方数でない，(ii) 次の二つのうちいずれかを満たす：

$$(\mathrm{ii}-1) \quad uw \equiv 1 \pmod 3$$

$$(\mathrm{ii}-2) \quad 3 \nmid w,\ u \equiv w \equiv \pm 2 \pmod 5.$$

このとき，$Z^3 - uwZ - u^2$ は必ず既約になり，従って，$\mathbb{Q}(\sqrt{d})$ の類数は 3 で割れる．

また，特に $u := a^4 p_1^{4\alpha_1 - 3} \cdots p_r^{4\alpha_r - 3}$，$w := 4b$ とれば，これは Ohta [7] の与えた部分族である．

このように以前から類数が 3 で割れる二次体の部分族が与えられてきた．これ以外にも，何か面白い部分族はないだろうか．そこで次の例を考える．

例 5. 平方数でない整数 D が次のように表されたとする：

$$27b^2D = 4m^3 - a^2 \tag{2.1}$$

但し，a，b，m は互いに素な 0 でない整数．このとき，多項式 $f(X) = X^3 - 3mX - a$ が $\mathbb{Q}$ 上既約ならば，$\mathbb{Q}(\sqrt{D})$ の類数は 3 で割れる．

証明. これは、主定理で $u = a^2$，$w = 3m$ とおいた場合である． □

式 (2.1) は次のように変形できる：

(2.2)

$$m^3 = \frac{a^2 + 27b^2D}{4} = N_{\mathbb{Q}(\sqrt{-3D})/\mathbb{Q}}\alpha, \quad \alpha = \frac{a + 3b\sqrt{-3D}}{2} \in \mathbb{Q}(\sqrt{-3D}).$$

従って，どんな D に対しても解 a，b，m は存在する．実は簡単な計算で次がわかる．

補題 1.

$$\alpha : \mathbb{Q}(\sqrt{-3D}) \text{で立方数} \iff f(X) : \mathbb{Q} \text{上可約}$$

立方数ではないが，ノルムをとると立方数になる二次体の元は，3 乗して初めて単項になるイデアル $\mathfrak{a}$ に対する $\alpha = \mathfrak{a}^3$ か，または，$D < 0$ ならば基本単数 ε に対する $\alpha = \varepsilon^{3n \pm 1}$ である．ここで，次の定理がある：

定理. (Herz [3]) 虚二次体 $k := \mathbb{Q}(\sqrt{d})$ に対して, 実二次体 $k' := \mathbb{Q}(\sqrt{-3d})$ の類数, 基本単数をそれぞれ h', ε とする. このとき, k の類数が 3 で割れるための必要十分条件は, 次の条件のうち, 少なくともいずれか一つが成り立つことである:

$$\text{(i)}\ \ N_{k'/\mathbb{Q}}\,\varepsilon = 1,\ \ Tr_{k'/\mathbb{Q}}\,\varepsilon \equiv \pm 2\ (27)$$

$$\text{(ii)}\ \ Tr_{k'/\mathbb{Q}}\,\varepsilon \equiv 0\ (9)$$

$$\text{(iii)}\ \ N_{k'/\mathbb{Q}}\,\varepsilon = -1,\ \ Tr_{k'/\mathbb{Q}}\,\varepsilon \equiv \pm 4\ (9)$$

$$\text{(iv)}\ \ 3 \mid h'.$$

もし実二次体 k' の類数が 3 で割れなければ, 3 乗して初めて単項になるイデアルはない. しかしそのときはこの定理より, (i), (ii), (iii) の条件のどれかを満たしており, そして実際 (i) を満たしているときは ε を, (ii) を満たしているときは ε^2 を, (iii) を満たしているときは ε^4 を α ととると, 式 (2.2) を満たしていることがわかる. つまり, k' の類数が 3 で割れないときは, 必ず基本単数から k 上の 3 次不分岐アーベル拡大が作られる訳である. 鏡像定理 (Scholz [8]) より, 虚二次体 k のイデアル類群の 3-rank と実二次体 k' のイデアル類群の 3-rank との差は多くても 1 であるが, その差が基本単数と関係しているということが, この例からもわかる.

References

[1] J. Brinkhuis, *Normal Integral Bases and the Spiegelungssatz of Scholz*, Acta Arithmetica **69** (1995), 1–9.

[2] P. Hartung, *Explicit Construction of a Class of Infinitely Many Imaginary Quadratic Fields Whose Class Number is Divisible by* 3, J. Number Theory **6** (1974), 279–281.

[3] C. S. Herz, *Seminer on Complex Multiplication*, VII. Construction of class fields, Springer-Verlag, Berlin-Heidelberg-New York, 1966.

[4] T. Honda, *On Real Quadratic Fields whose Class Numbers are Multiples of* 3, J. Reine Angew. Math. **233** (1968), 101–102.

[5] Y. Kishi and K. Miyake, *Characterization of the Quadratic Fields whose Class Numbers are Divisible by Three*, Tokyo Met. Univ. Math. Pre. Ser. (1997), no. 7.

[6] Tr. Nagel, *Über die Klassenzahl imaginär-quadratischer Zahlköper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.

[7] K. Ohta, *On Algebraic Number Fields whose Class Numbers are Multiples of* 3, Bull. Fac. Gen. Ed. Gifu Univ. **1981** (1982), 51–54.

[8] A. Scholz, *Über die Beziehung der Klassenzahl quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203.